# CTL – Computation Tree Logic
# a Logic for Branching-time Model Checking[1]

Paul Jackson
Paul.Jackson@ed.ac.uk

University of Edinburgh

Formal Verification
Autumn 2023

[1] Including contributions by Jacques Fleuriot, Bob Atkey and Elizabeth Polgreen

# CTL Syntax

Assume some set Atom of atomic propositions

$$\begin{aligned}\phi, \psi ::= \quad & p \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \Rightarrow \psi \mid \\ & \mathbf{AX}\,\phi \mid \mathbf{EX}\,\phi \mid \mathbf{AF}\,\phi \mid \mathbf{EF}\,\phi \mid \mathbf{AG}\,\phi \mid \mathbf{EG}\,\phi \mid \\ & \mathbf{A}[\phi\,\mathbf{U}\,\psi] \mid \mathbf{E}[\phi\,\mathbf{U}\,\psi]\end{aligned}$$

where $p \in$ Atom

Each temporal connective is a pair of a path quantifier

**A** — for all paths

**E** — there exists a path

and an LTL-like temporal operator **X**, **G**, **F** or **U**

Precedence high-to-low:
(**AX**, **EX**, **AF**, **EF**, **AG**, **EG**, $\neg$),
($\wedge$, $\vee$),
$\Rightarrow$

# CTL Semantics 1: Transition Systems and Paths

(This is the same as for LTL)

### Definition (Transition System)

A transition system $\mathcal{M} = \langle S, \rightarrow, L, I \rangle$ consists of

| | | | |
|---|---|---|---|
| $S$ | | | set of states |
| $\rightarrow$ | $\subseteq$ | $S \times S$ | transition relation |
| $L$ | $:$ | $S \rightarrow \mathcal{P}(\mathrm{Atom})$ | labelling function |
| $I$ | $\subseteq$ | $S$ | set of initial states (*sometimes*) |

such that $\forall s. \exists t.\ s \rightarrow t$.

### Definition (Path)

A path $\pi$ in a model $\mathcal{M} = \langle S, \rightarrow, L, I \rangle$ is an infinite sequence of states $s_0, s_1, \ldots$ such that $s_0 \in I$ and $\forall i \geq 0.\ s_i \rightarrow s_{i+1}$.

# CTL Semantics 2: Satisfaction relation

Satisfaction relation $\mathcal{M}, s \models \phi$ read as
*"state s in model M satisfies CTL formula $\phi$".*

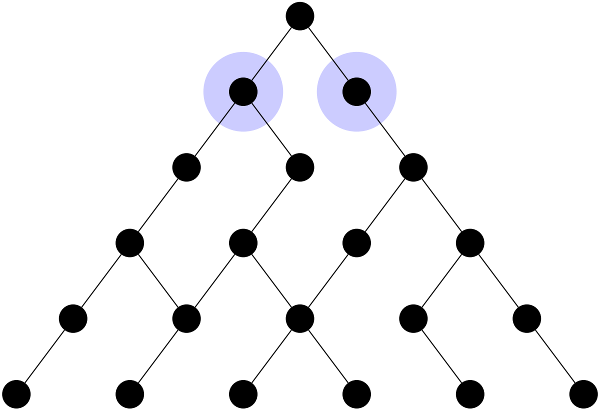
The $\mathcal{M}$ is often implicit.

$$
\begin{array}{lll}
s \models \top & & \\
s \not\models \bot & & \\
s \models p & \text{iff} & p \in L(s) \\
s \models \neg\phi & \text{iff} & s \not\models \phi \\
s \models \phi_1 \wedge \phi_2 & \text{iff} & s \models \phi_1 \text{ and } s \models \phi_2 \\
s \models \phi_1 \vee \phi_2 & \text{iff} & s \models \phi_1 \text{ or } s \models \phi_2 \\
s \models \phi_1 \Rightarrow \phi_2 & \text{iff} & s \models \phi_1 \text{ implies } s \models \phi_2
\end{array}
$$

# CTL Semantics 3: Satisfaction relation (continued)

| | | |
|---|---|---|
| $s \models \mathbf{AX}\,\phi$ | iff | $\forall\ s'.\ s \to s'$ implies $s' \models \phi$ |
| $s \models \mathbf{EX}\,\phi$ | iff | $\exists\ s'.\ s \to s'$ and $s' \models \phi$ |
| $s \models \mathbf{AG}\,\phi$ | iff | $\forall$ paths $\pi$ s.t. $s_0 = s.\ \forall i.\ s_i \models \phi$ |
| $s \models \mathbf{EG}\,\phi$ | iff | $\exists$ path $\pi$ s.t. $s_0 = s.\ \forall i.\ s_i \models \phi$ |
| $s \models \mathbf{AF}\,\phi$ | iff | $\forall$ paths $\pi$ s.t. $s_0 = s.\ \exists i.\ s_i \models \phi$ |
| $s \models \mathbf{EF}\,\phi$ | iff | $\exists$ path $\pi$ s.t. $s_0 = s.\ \exists i.\ s_i \models \phi$ |
| $s \models \mathbf{A}[\phi_1\ \mathbf{U}\ \phi_2]$ | iff | $\forall$ paths $\pi$ s.t. $s_0 = s.$ <br> $\exists i.\ s_i \models \phi_2$ and $\forall j < i.\ s_j \models \phi_1$ |
| $s \models \mathbf{E}[\phi_1\ \mathbf{U}\ \phi_2]$ | iff | $\exists$ path $\pi$ s.t. $s_0 = s.$ <br> $\exists i.\ s_i \models \phi_2$ and $\forall j < i.\ s_j \models \phi_1$ |

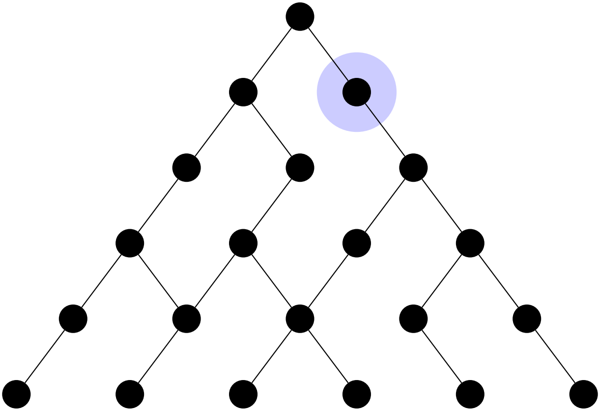
# CTL in Pictures



**AX** $\phi$

For *every* next state, $\phi$ holds.

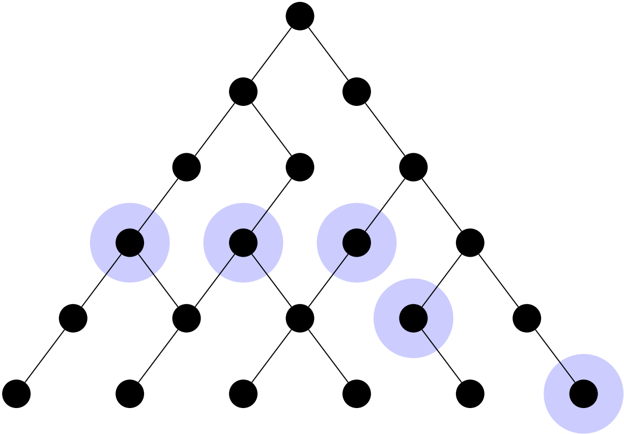
# CTL in Pictures



**EX** $\phi$

There *exists* a next state where $\phi$ holds.

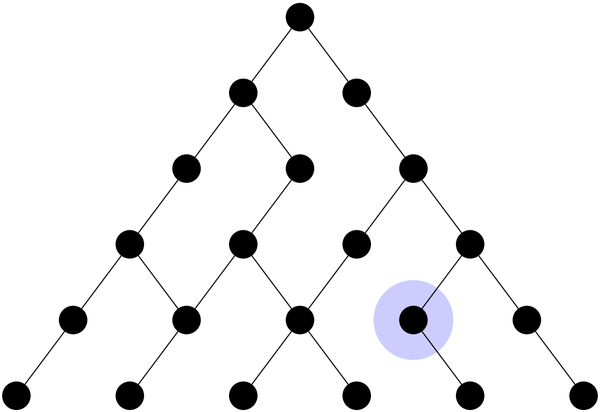
# CTL in Pictures



**AF** $\phi$

For all paths, there exists a future state where $\phi$ holds.

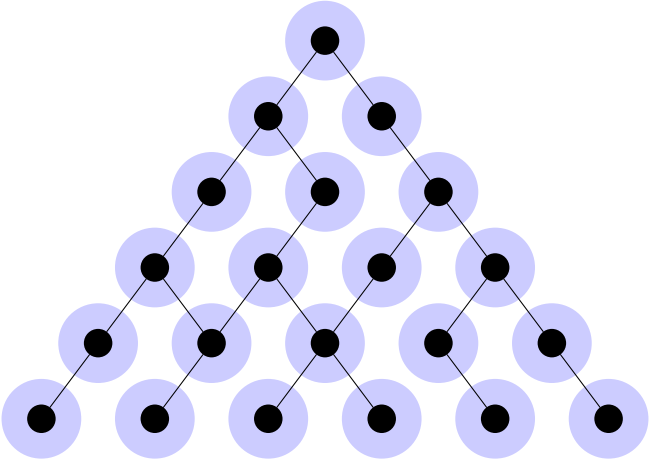
# CTL in Pictures



**EF** $\phi$

There exists a path with a future state where $\phi$ holds.

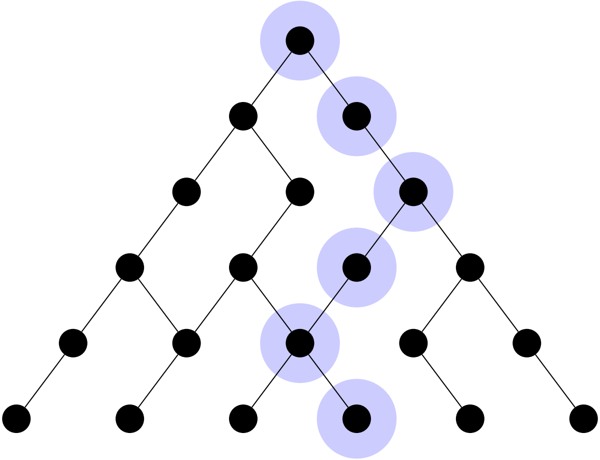
# CTL in Pictures



**AG** $\phi$

For all paths, for all states along them, $\phi$ holds.

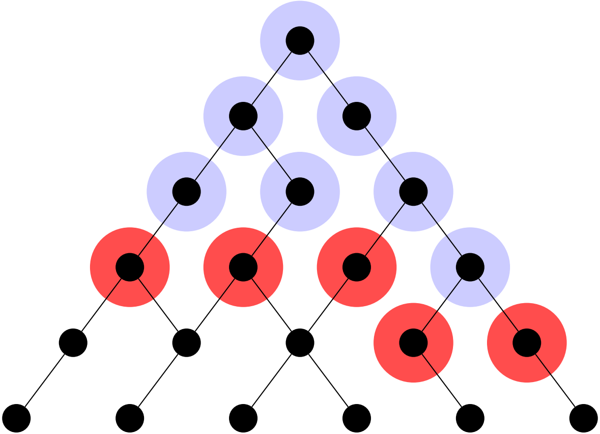
# CTL in Pictures



**EG** $\phi$

There exists a path such that, for all states along it, $\phi$ holds.

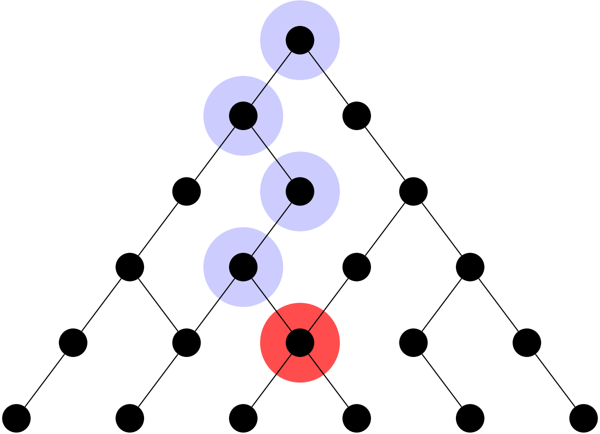
# CTL in Pictures



$\mathbf{A}[\phi \; \mathbf{U} \; \psi]$

For all paths, $\psi$ eventually holds, and $\phi$ holds at all states earlier.

# CTL in Pictures



$$\mathbf{E}[\phi\ \mathbf{U}\ \psi]$$

Exists path where $\psi$ eventually holds, and $\phi$ holds at all states earlier.

# CTL Examples

- **EF** $p$
  There exists a path along which p eventually holds
- **AG AF** $p$
  In all future states, it is always the case that p eventually holds
- **AG** $(p \Rightarrow \mathbf{AF}\, q)$
  In all future states, if p holds then always eventually q holds

# CTL Examples (continued)

- $\mathbf{AG}\,(p \Rightarrow \mathbf{E}[p\,\mathbf{U}\,q])$
  In all future states, if p holds then there exists a path onwards along which p continues to hold until q holds

- $\mathbf{AG}\,(p \Rightarrow \mathbf{EG}\,q)$
  In all future states, if p holds then there exists a path onwards along which p holds forever

- $\mathbf{EF}\,\mathbf{AG}\,p$
  There exists some future state from which p always holds along all paths

# CTL Equivalences

de-Morgan dualities for the temporal connectives

$$\begin{aligned}
\neg \mathbf{EX}\,\phi &\equiv \mathbf{AX}\,\neg\phi \\
\neg \mathbf{EF}\,\phi &\equiv \mathbf{AG}\,\neg\phi \\
\neg \mathbf{EG}\,\phi &\equiv \mathbf{AF}\,\neg\phi \\
\neg \mathbf{EX}\,\phi &\equiv \mathbf{AX}\,\neg\phi
\end{aligned}$$

Also have

$$\begin{aligned}
\mathbf{AF}\,\phi &\equiv \mathbf{A}[\top\;\mathbf{U}\;\phi] \\
\mathbf{EF}\,\phi &\equiv \mathbf{E}[\top\;\mathbf{U}\;\phi] \\
\mathbf{A}[\phi_1\;\mathbf{U}\;\phi_2] &\equiv \neg(\mathbf{E}[\neg\phi_2\;\mathbf{U}\;(\neg\phi_1 \wedge \neg\phi_2)] \vee \mathbf{EG}\,\neg\phi_2)
\end{aligned}$$

From these one can show that sets $\{\mathbf{AU}, \mathbf{EU}, \mathbf{EX}\}$ and $\{\mathbf{EG}, \mathbf{EU}, \mathbf{EX}\}$ are both adequate sets of temporal connectives.

# Differences between LTL and CTL

- LTL allows for questions of form
  - *For all paths, does LTL property $\phi$ hold?*
  - *Does there exist a path on which LTL property $\phi$ holds?* (Ask whether $\neg\phi$ holds on all paths and look for a counter-example)
- CTL allows mixing of path quantifiers
  - $\mathbf{AG}\,(p \Rightarrow \mathbf{EG}\,q)$
- Some path properties are impossible to express in CTL.
  - In LTL: $\mathbf{G}\,\mathbf{F}\,p \Rightarrow \mathbf{G}\,\mathbf{F}\,q$
  - In CTL: $\mathbf{AG}\,\mathbf{AF}\,p \Rightarrow \mathbf{AG}\,\mathbf{AF}\,q$ is *not* the same. (Consider a model in which $p$ holds infinitely often on some paths, but not all, and $q$ holds nowhere)
  - Core issue: $\Rightarrow$ in CTL cannot be used to restrict paths
- Exist *Fair CTL* refinements of CTL that address this issue to some extent
  - E.g. path quantifiers can be restricted to consider only paths on which given properties hold infinitely often.

# Fairness

- Key in modelling concurrent systems
- Concurrency handled using Interleaving:

$$\begin{aligned}(s_1, s_2) \longrightarrow (s_1', s_2') \;\; &\doteq \;\; (s_1 \longrightarrow_1 s_1' \wedge s_2 = s_2') \vee \\ & \quad\;\; (s_1 = s_1' \wedge s_2 \longrightarrow_2 s_2')\end{aligned}$$

- But want to avoid considering paths in which only one process ever runs
- E.g. in LTL prove properties of form

$$\mathsf{Fair} \Rightarrow \phi$$

where

$$\mathsf{Fair} \;=\; (\mathbf{G}\,\mathbf{F}\,\mathsf{taken}_1) \wedge (\mathbf{G}\,\mathbf{F}\,\mathsf{taken}_2)$$

and $\mathsf{taken}_i$ holds at a state of a path if process $i$ takes a step from that state to the next state.

# Further difference between LTL and CTL

The LTL formula

$$\mathbf{F}\,\mathbf{G}\,p$$

and the CTL formula

$$\mathbf{AF}\,\mathbf{AG}\,p$$

are not the same.

*Exercise:* give a model which satisfies one of the formulas but not the other.

# CTL*

- Extends both LTL and CTL
- *State* formulas, evaluated in states:

$$\begin{aligned} \phi ::= \quad & p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \Rightarrow \phi \mid \\ & \mathbf{A}[\alpha] \mid \mathbf{E}[\alpha] \end{aligned}$$

- *Path* formulas, evaluated along paths:

$$\begin{aligned} \alpha ::= \quad & \phi \mid \neg\alpha \mid \alpha \wedge \alpha \mid \alpha \vee \alpha \mid \alpha \Rightarrow \alpha \mid \\ & \mathbf{X}\,\alpha \mid \mathbf{F}\,\alpha \mid \mathbf{G}\,\alpha \mid \alpha\,\mathbf{U}\,\alpha \end{aligned}$$

- An LTL formula $\alpha$ is expressed as $\mathbf{A}[\alpha]$ in CTL*
- Harder to model check

# Further Reading


- M.Y. Vardi, *Branching vs. Linear Time: Final Showdown*. Tools and Algorithms for the Construction and Analysis of Systems, LNCS vol. 2031, pp 1-22, 2001
- Michael Huth and Mark Ryan. *Modelling and Reasoning about Systems*, 2nd Edition, 2004. Sections 3.4 and 3.5.